REMARKS

Reconsideration and withdrawal of the rejections set forth in the Office Action dated July 6, 2005 are respectfully requested. Applicant would like to thank the Examiner for the interview with Applicant's representative on October 5, 2005. During the interview, the parties discussed the cited references, the independent claims, and embodiments of the invention.

Claims 1-5, 18-28 and 30 are pending in this application. Claims 6-17 and 31-33 have been cancelled and will be pursued in a divisional application. Claim 29 has been canceled and incorporated into claim 25. Claims 1, 18, 19, 21-25, 27, and 30 have been amended.

Rejections Under 35 U.S.C. § 112

Claims 1-5 and 18-30 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. The claims have been amended to satisfy the concerns of the Examiner.

Rejections Under 35 U.S.C § 103

Claims 1-5 and 18-30 stand rejected under 35 U.S.C. 103(a) as being unpatentable according to the following chart:

Claims 25-27 and 30	Malek in view of Lynn
Claim 1	Malek in view of Lynn and Chien
Claim 2	Malek, Lynn, Chien, and Bender
Claims 3-5, 18-21 and 23	Malek, Lynn, Chien, and Schneier

Claim 22	Malek, Lynn, Chien, Schneier, and Dent
Claim 24	Malek, Lynn, Chien, Schneier, Bender and "NetBEUI"
Claim 28	Malek, Lynn, and Schneier
Claim 29	Malek, Lynn, and Dent

1. Independent Claim 25

Claim 25 has been amended to incorporate the subject matter of original claim 29 and to recite the dual functionality of a control message within the wireless system. Amended claim 25 stands rejected as being unpatentable over Malek in view of Lynn, and further in view of Dent. Applicant respectfully disagrees.

As the Examiner is aware, in order to make a *prima facie* case for obviousness, the cited references "must teach or suggest all the claim limitations" and "the claimed invention as a whole must be considered" and "the references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination" (MPEP 2142).

A. The cited references do not teach or suggest all the claim limitations

Amended claim 25 recites, among other elements, an apparatus for synchronizing an encryption and/or decryption process comprising "encryption synchronization means configured to detect a particular control message in a data transmission wherein the particular control message is used according to a wireless communication protocol to provide at least one other control function under the wireless communication protocol, and, in response, initiate an encryption and/or decryption process" (Emphasis added).

Since wireless systems notify base stations and/or remote units to begin encrypting and/or decrypting bit streams, it is beneficial to initiate an encryption and/or decryption process upon detecting a control message, as a control message is sent before completing a connection establishment process and just before transmission of telephony data. The control message, therefore, indicates an ideal time to begin encryption synchronization of telephony data. Because such systems already use control messages to transmit control and other information, it is advantageous to provide a system that gives control messages dual functionality, the additional functionality being that of indicating an ideal time to begin an encryption and/or decryption process.

The office action relies on column 4, lines 47-57 of Malek to allegedly disclose "encryption synchronization means configured to detect a particular control message in a data transmission, and in response, wherein the particular control message occurs just before the transmission of telephony data." (Applicant assumes the phrase "and in response" is misplaced). Applicant respectfully submits that Malek does not provide such a disclosure.

Malek is directed to an encryption technique that does not degrade the voice quality of a transmission. Malek uses a TDMA/TDD frame 201 that comprises time slots 202 for FCU (fixed control unit) transmission and time slots 203 for PCU (portable control unit) transmission. Malek describes the time slots as having "a synchronization part 204 comprising a synchronization marker for synchronizing a linked PCU and FCU, and a data part 205," wherein the data part 205 comprises a "control part 206 for passing control information" (column 4, lines 48-54). The system of Malek uses the synchronization part and the control part to synchronize the encryption and decryption of information carried in a user data part 208, but does not use these parts to initiate an encryption or decryption process. Malek discloses that "in operation, frame synchronization portions of TDMA/TDD circuits within the FCU 102 and in the PCU 120 enable the encryption and decryption of the information during the transmission of the user data part 208 and during the transmission of the control part 206 when the control part comprises user signaling

information. The TDMA/TDD circuits disable the encryption and decryption during all other parts of the transmission" (column 5, lines 2-11). Therefore, the encryption and decryption process of Malek occurs "during the transmission of the user part" and "during the transmission of the control part when the control part comprises user signaling an information," and does not "detect a particular control message" nor "initiate encryption and/or decryption" in response to such messages. In sum, the encryption and decryption process of Malek does not consider control messages when beginning encryption of data transmissions.

The office action admits that Malek "fails to disclose initiating an encryption/decryption process," and relies on Lynn to satisfy this element, merely reciting that "Lynn teaches initiating an encryption/decryption system," in column 2, lines 54-64. These lines, however, discuss an Initialization Vector used to produce a temporal key which becomes an input for a pseudorandom (PN) number generator that produces a unique PN sequence of binary digits. Lynn discusses encryption techniques, such as the generation of PN numbers based in a number of inputs (e.g. an Initialization Value), and does not discuss the initialization of encryption and/or decryption processes.

Neither Malek nor Lynn disclose initiating an encryption and/or decryption process in response to detecting a particular control message in a data transmission, wherein the particular control message is used according to a wireless communication protocol to provide at least one other control function under the wireless communication protocol

Dent discloses a system for the synchronization of encryption devices using a multi-bit counter and a pseudo-random keystream. The office action relies on Dent merely to provide a disclosure of "at least one access or control channel" (column 6, lines 44-45). However, Dent, like Malek and Lynn, does not describe or suggest initiating an encryption and/or decryption process in response to detecting a particular control message in a data transmission. In sum, claim 25 as amended is allowable.

B. There is no suggested desirability in combining the cited references

The office action relies on the ability of Lynn to provide self-synchronization as motivation to combine Malek with Lynn. Lynn discloses the selective reuse of pseudorandom encoding sequences, and explains that a "drawback of the prior art system is that the receiver's PN generator may lose synchronization with that of the transmitter under some circumstances" and "it is therefore desirable that a high speed cryptosystem exhibit the property of self-synchronization between transmitter and receiver such that no additional recovery procedures are required to decode messages" (column 2, lines 34-51). According to Lynn, self-synchronization provides everything needed to decode a block of transmitted data within a transmitted message, and that knowledge of prior messages or sequences is not required (column 7, lines 20-30).

Malek, however, is not directed towards a method of preventing the loss of synchronization between a transmitter and a receiver, but towards a method of maintaining encryption and decryption in a wireless system throughout a hand-off. Malek seeks to remedy previous techniques of maintaining encrypted data during hand-off by providing a continuation value being a "value expected in the portable communication unit encryption synchronization counter concurrent with hand-off completion" (column 2, lines 35-38). The goal of Malek is to provide a solution to the problem of losing encrypted information during hand-off.

Additionally, and possibly more important, Malek describes an ability of effecting a synchronized encryption and decryption between a receiver and a transmitter. For example, Malek discloses "generating a single encryption sequence for controlling the synchronized encryption and decryption occurring in the FCU 102 [fixed communication unit] and the PCU 120 [portable communication unit]" (column 8, lines 40-48). Malek, therefore, describes synchronized encryption between a receiver and a transmitter, and therefore, would have no use for the self-synchronization techniques of Lynn. Therefore, for at least the reasons stated above, it would not be desirable to combine the Malek

reference with the Lynn reference and one of ordinary skill in the art would not be motivated to make such a combination.

The cited references do not "teach or suggest" all the claim limitations, nor is there any motivation or suggestion to combine the cited references, and therefore for at least these reasons, amended claim 25 is not obvious in view of the combination of Malek and Lynn (and Dent).

2. Independent claim 1

Claim 1 stands rejected as being unpatentable over Malek in view of Lynn, and further in view of Chien. Applicant respectfully disagrees.

Claim 1 recites similar elements to amended claim 25, such as "determining whether the control data contains a particular control message, if the control data contains the particular control message, loading an encryption synchronization counter with a number of control message bytes to be transmitted and initializing the encryption synchronization counter," and "determining whether the control data contains the particular control message, if the control data contains the particular control message, initializing the cryptosystem using the key" (emphasis added).

The office action refers to the combination of Malek and Lynn to allegedly disclose all the elements except for the element of "the use of an encrypted airlink packet," and relies on Chien to provide such an element. However, as discussed earlier with respect to amended claim 25, the combination of Malek and Lynn does not disclose all the elements of the claim, as it does not disclose the elements relating to the initializing of an encryption synchronization counter based on a particular control message.

Chien is directed to a method of reducing traffic over a communication link, and not to encryption and/or decryption systems. The office action relies on Chien merely to provide a disclosure of "an encrypted airlink packet" (paragraph 81). Chien, therefore,

does not describe or suggest the element of initializing an encryption and/or decryption process based on a particular control message in a data transmission.

Therefore, applicant respectfully contends that claim 1 is obvious over the combination of Malek, Lynn and Chien for at least the reasons stated above.

3. Independent claim 18

Claim 18 stands rejected as being unpatentable over Malek in view of Lynn, Chien and Schneier. Applicant respectfully disagrees.

Claim 18 recites similar elements to that of claim 1 and amended claim 25, including the element of "detecting a particular control message that passes through an associated control channel in the blocks of data for initiating encryption, wherein the particular control message is used according to a wireless communication protocol to provide at least one other control function under the wireless communication protocol" and "in response to detecting, loading a size of the message for transmission into a counter, wherein the counter reaches zero when all of the blocks in the message for transmission have been sent" (emphasis added).

The office action refers to the combination of Malek, Lynn and Chien to allegedly disclose all the elements except for the element of "the use of a state box," and relies on Schneier to provide such an element. However, as discussed earlier with respect to amended claim 25, the combination of Malek and Lynn does not disclose all the elements of the claim, as it does not disclose the elements relating to loading a size of the message for transmission into a counter in response to detecting particular control message.

Schneier is directed to encryption techniques, such as real random-sequence generators, and not over encryption systems. The office action relies on Schneier merely to provide a disclosure of "a state box " (page 398). Schneier, therefore, does not describe

or suggest the element of loading a size of the message for transmission into a counter in response to detecting particular control message.

Therefore, applicant respectfully contends that claim 1 is obvious over the combination of Malek, Lynn, Chien and Schneier for at least the reasons stated above.

4. Dependent claims 2-5, 19-24, 26-38 and 30

Since claims 2-5, 19-24, 26-28 and 30 depend from claims 1, 18 or 25, they are patentable for at least the reasons stated with respect to the independent claims.

5. Conclusion

Overall, the applicant respectfully submits that independent claims 1, 18 and 25 are patentable over the applied references. Since these independent claims are allowable, based on at least the above reasons, the claims that depend from them are likewise allowable.

In view of the foregoing, the claims pending in the application comply with the requirements of 35 U.S.C. § 112 and patentably define over the applied art. A Notice of Allowance is, therefore, respectfully requested. If the Examiner has any questions or believes a telephone conference would expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-3090.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-0665, under Order No. 364388032US1 from which the undersigned is authorized to draw.

Dated: October 6, 2005

Respectfully submitted,

By _____

Michael J. Smith
Registration No.: 56,702
PERKINS COIE LLP/CW
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000
(206) 359-7198 (Fax)
Representative for Applicant